

UNITED STATES DISTRICT COURT  
DISTRICT OF SOUTH CAROLINA  
GREENVILLE DIVISION

In the Matter of the Search of

SEARCH WARRANT

Residence located at 107 Silver Ridge Court,  
Greer, South Carolina, more fully described below

Criminal Number 6-08-587

TO: Robert G. Hamod, Special Agent, Federal Bureau of Investigation, and any other Authorized Officer of the United States:

Affidavit(s) having been made before me by Robert G. Hamod, who has reason to believe that on the premises known as the residence located at 107 Silver Ridge Court, Greer, South Carolina, described as a single family two story residence with yellow/beige siding, white trim, black shutters, and the numbers "107" on the mailbox in front of the house, located by turning off Locust Hill Road (South Carolina Highway 290) onto North Rutherford Road and then left onto Silver Ridge Court, the house being approximately one quarter mile on the left, in the District of South Carolina, there is now concealed a certain person or property, namely records and evidence of the crimes of installing spy software on computers without authorization and of obtaining information from a protected computer without authorization, including: (a) any computer, and associated hardware and peripherals, which may have been used as an instrumentality in the offense; (b) records relating to user names, passwords, screen shots, e-mails, or other information that appears to have been obtained from computers operated or controlled by Joe Kernell, Butch Kirven, or members of the Greenville County Council; (c) records relating to "Remote Spy," remotespys.com, or spy software; (d) correspondence in any form pertaining to the unauthorized access to a computer; (e) records evidencing ownership or control of any computer or other data storage media seized pursuant to this warrant; and (f) records relating to or embodying passwords, password files, test keys, encryption codes, or other information necessary to access computer equipment, storage devices, or data seized pursuant to this warrant; as used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as hard disks, thumb drives, or other media that can store data); any handmade form (such as writing, drawing, painting); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies); I am satisfied that the affidavit(s) and any recorded testimony establish probable cause to believe that the person or property so described is now concealed on the person or premises above-described and establish grounds for the issuance of this warrant.

YOU ARE HEREBY COMMANDED to search on or before June 18, 2008 for the person or property specified, serving this warrant and making the search in the daytime - 6:00 a.m. to 10:00 p.m. / ~~at any time in the day or night as I find reasonable cause has been established,~~ and if the person or property be found there to seize same, leaving a copy of this warrant and receipt for the person or property taken, and prepare a written inventory of the person or property seized and promptly return this warrant to Bruce H. Hendricks, United States Magistrate Judge, as required by law.

Nighttime search specifically authorized:  Yes  No

Issued 1:55 p.m., June 10, 2008, at Greenville, South Carolina.

Bruce H. Hendricks  
United States Magistrate Judge

Bruce H. Hendricks  
Signature of Judicial Officer

# RETURN

Date Warrant Received

6/10/08

Date and Time Warrant Executed

6/10/08 5:15pm

Copy of Warrant and Receipt for Items Left With

TONY TROUT

Inventory Made in the Presence of

TONY TROUT

Inventory of Person or Property Taken Pursuant to the Warrant

- GATEWAY 832GM S/N SL5341004646
- GATEWAY MEATXPNT ESX 500S S/N 0028198986
- HP PAVILION ELITE M9040N S/N CNH741148G
- HP LAPTOP COMPAQ NC6320 S/N GNU622067B
- BLACK LAPTOP CARRYING CASE LABELED "HP INVENT" WITH POWERCORD
- BLACK NOTEBOOK PORTFOLIO CONTAINING MISC. PAPERS
- WESTERN DIGITAL HARD DRIVE S/N WCALA1990883 WITH POWER..CORD AND CONNECTOR CABLE
- NETGEAR USB DEVICE S/N 16525CBX1326B
- SEAGATE HARD DRIVE S/N .3QD0EP2J
- IPAQ POCKET PC S/N 00023-517-042-341
- IPAQ POCKET PC S/N 00023-517-969-917
- HP POCKET MEDIA DRIVE MODEL PD1600S S/N GNU7372DPK
- MAXTOR EXTERNAL HARD DRIVE S/N 2HA12MS8 WITH CONNECTOR CABLE
- DELL LATITUDE D620 LAPTOP S/N 4324A-BRCM1019
- BLACK LAPTOP CARRYING CASE LABELED "DELL" WITH POWER CORD


## CERTIFICATION

I swear that this inventory is a true and detailed account of the person or property taken by me on the warrant.




---

Subscribed, sworn to, and returned before me this date.




---

U. S. District Judge or Magistrate Judge

6-12-08

Date

6:08-587

**A F F I D A V I T**

I, ROBERT G. HAMOD, being duly sworn hereby depose and state:

I am a duly appointed Special Agent of the FBI currently assigned to the Greenville, South Carolina, Resident Agency and have been so employed for the past sixteen years. Upon accepting a position with the FBI, your affiant underwent an extensive sixteen week training course involving investigations of federal crimes, to include Computer Intrusion. Your affiant has personally been involved with the investigation of Harold Anthony Trout, also known as Tony Trout, in the Greenville, South Carolina area involving computer intrusion.

The statements contained in this affidavit are based in part on information provided by witnesses and State Law Enforcement Officers. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that evidence of violations of Title 18, United States Code, Section 1030 are located at 107 Silver Ridge Court, Greer, South Carolina.

**STATUTORY AUTHORITY**

This investigation concerns alleged violations of Title 18, United States Code, Sections 1030(a)(2)(C), concerning the unauthorized access of a computer.

**SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS**

Based upon your Affiant's knowledge, training and experience, and the experience of other law enforcement personnel, your Affiant knows that searches and seizures of evidence from computers commonly require agents to seize most or all computer items (hardware, software, and instructions) to be processed later by a qualified computer expert in a laboratory or other controlled environment. This is almost always true because of the following:

Computer storage devices (like hard drives, diskettes, tapes, laser disks, and others) can store the equivalent of thousands of pages of information. Especially when the user wants to conceal criminal evidence, he or she often stores it in random order with deceptive file

names. This requires searching authorities to examine all the stored data to determine whether it is included in the warrant. This sorting process can take weeks or months, depending on the volume of data stored, and it would be impractical to attempt this kind of data search on site; and

Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert should analyze the system and its data. The search of a computer system is an exacting scientific procedure which is designed to protect the integrity of the evidence and to recover even "hidden," erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to tampering or destruction (both from external sources or from destructive code imbedded in the system as a "booby trap"), the controlled environment of a laboratory is essential to its complete and accurate analysis.

In order to fully retrieve data from a computer system, the analyst needs all magnetic storage devices as well as the central processing unit (CPU). In addition, the analyst needs all the system software (operating systems or interfaces, and hardware drivers) and any applications software which may have been used to create the data (whether stored on hard drives or on external media).

In addition, there is probable cause to believe that the computer and its storage devices, the monitor, keyboard, and modem are all instrumentalities of the crimes of unauthorized access of a computer in violation of law, and should all be seized as such.

#### DEFINITIONS

The term "computer," as used herein, is defined pursuant to Title 18, United States Code, Section 1030(e)(1), as "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device."

Your Affiant knows that computer hardware and computer software may be utilized to store records which include but are not limited to those relating to business activities, criminal activities, associate names and addresses and the identity and location of assets illegally gained through criminal activity.

The terms "records," "documents," and "materials" include all information recorded in any form, including electronic, visual or aural, and including the originals and all non-identical copies thereof, whether different from the original by reason of any notation made on such copies or otherwise, including, but not limited to the following:

Written or printed matter of any kind, correspondence, memoranda, notes, diaries, statistics, letters, telephone toll records, telegrams, contracts, reports, checks, statements, receipts, summaries, pamphlets, books, ledgers, journals, registers, records, vouchers, slips, bills, calendars, pads, notebooks, files, logs, lists, bulletins, credit materials, data bases, teletypes, telefaxes, invoices, worksheets;

Graphic records or representations, photographs, slides, drawings, designs, graphs, charts, pictures, sketches, images, films, videotapes; and aural records or representations, tapes, records, discs.

The terms "records," "documents," and "materials" include all of the foregoing in whatever form and by whatever means the records, documents, or materials, their drafts, or their modifications may have been created or stored, including (but not limited to) any handmade form (such as writing, drawing, painting, with any implement on any surface directly or indirectly); any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies); any mechanical form (such as phonograph records, printing, or typing); any electrical, electronic, or magnetic form (such as tape recordings, cassettes, compact discs, or any information on an electronic or magnetic storage device, such as floppy diskettes, hard disks, hard drives, CD-ROMs, optical discs, printer buffers, smart cards, memory calculators, electronic dialers, Bernoulli drives, or electronic notebooks, as well as printouts or readouts from any magnetic storage device).

The term "Internet Service Provider" (ISP) refers to an entity which provides access to a host computer, from which electronic contact can be made to literally millions of computers

around the world. A host computer is one that is attached to a dedicated network and serves many users. These host computers are sometimes commercial concerns, such as CompuServe and America-Online which allow subscribers to dial a local number and connect to a network which is in turn connected to their host systems. These service providers allow electronic mail service between subscribers and sometimes between their own subscribers and those of other networks.

The term "Internet Protocol" (IP) address is a unique identifier for a computer on a network. The format of an IP address is a 32-bit numeric address written as four sequences of numbers separated by periods.

### SOURCES OF INFORMATION

Information was received from a witness, who is in a position to obtain this information, that Tony Trout utilized a computer monitoring software which he surreptitiously implanted onto a computer owned by the County of Greenville, South Carolina but in the possession of Joe Kernell, County Administrator, to gain access to and obtain information from this computer. Trout is currently an elected Councilman for Greenville County, South Carolina. In his capacity as a councilman, Trout has made allegations of fraud against Kernell in regards to the granting of road paving contracts in the County of Greenville.

Sometime in April 2008, the witness had a meeting with Trout, at Trout's residence, in which Trout revealed that he had accessed Kernell's county computer. Trout explained to the witness that he had used a commercial software product called "Remote Spy" to access information on Kernell's computer. Trout was able to implant the software on Kernell's computer by first sending it attached to an e-mail to Butch Kirven, another County Councilman. Kirven then forwarded the e-mail to Kernell. When Kernell opened the e-mail the program was then installed on his computer. This software takes periodic screen shots of the target computer. It then sends this information to a server where the user can then gain access to it.

Trout then accessed his computer, in the presence of the witness, and showed him the information he had obtained. Included in this information was a log of the date/time that the screen shot was taken as well as a description of the item that was being viewed. The witness also viewed several of the screen shots which appeared to come from Kernell's computer concerning

county business. As well as this it appeared that Trout was able to obtain Kernell's user names and passwords for a number of accounts. Trout then printed copies of the screen shots that the two viewed and provided them to the witness. The witness provided these copies to your affiant.

Trout then told the witness that he had used the information gathered by the software on Kernell's computer to obtain Kernell's user name and password for his e-mail account. Trout used this information to access Kernell's e-mail account and download the information to his own computer. Trout showed several of the e-mails which he thought would be of interest to the witness. Trout also provided copies of these e-mails to the witness. The witness provided these copies to your affiant.

Trout has spoken to the witness several times about this matter. Trout has sent several more items obtained from Kernell to the witness via e-mail. The witness printed several of these items and provided them to your affiant.

The witness last saw Trout's computers, which he used to show the witness this information, at Trout's residence on June 7, 2008.

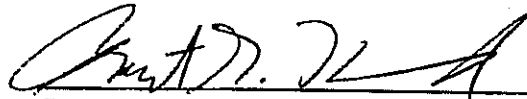
A check of the current telephone directory for Greenville, South Carolina shows a listing for Tony Trout, 107 Silver Ridge Court, Greer, South Carolina. A check of South Carolina Department of Motor Vehicles records showed a drivers license that lists Trout's address as 107 Silver Ridge Court, Greer, South Carolina. Your affiant drove by the residence and saw a red Ford Explorer in the garage. A check of South Carolina Department of Motor Vehicles records showed a 2005 Ford Explorer registered to Donna Trout 107 Silver Ridge Court, Greer, Anderson, South Carolina.

Based on the above information, I believe that there is probable cause to believe that Title 18, United States Code, Section 1030(a)(2)(C), which makes it a federal crime for any person to intentionally access a protected computer without authorization and obtain information from that computer using an interstate or international communication, has been violated.

The property and evidence believed to be concealed at 107 Silver Ridge Court, Greer, South Carolina is listed in attachment A to this affidavit which is incorporated by reference as if fully set forth herein. Your affiant requests authority to seize such material. In consideration of the foregoing, your affiant respectfully requests that this Court issue a search warrant for 107


Silver Ridge Court, Greer, South Carolina, authorizing the seizure of the items described in Attachment A. 107 Silver Ridge Court, Greer, South Carolina, is described as follows:

A single family two story residence, with yellow/beige siding, white trim and black shutters. The numbers "107" are located on the mailbox in front of the house. The house can be reached by turning off Locust Hill Road (South Carolina Highway 290) onto North Rutherford Road and then left onto Silver Ridge Court. The house is located approximately one quarter mile on the left.



ROBERT G. HAMOD, Special Agent  
Federal Bureau of Investigation

SUBSCRIBED TO AND SWORN TO  
BEFORE ME THIS TENTH DAY  
OF JUNE, 2008.



Bruce H. Hendricks  
UNITED STATES MAGISTRATE JUDGE

**ATTACHMENT A****LIST OF ITEMS TO BE SEIZED**

Records and evidence of the crimes of installing spy software on computers without authorization and of obtaining information from a protected computer without authorization, including:

- a. Any computer, and associated hardware and peripherals, which may have been used as an instrumentality in the offense;
- b. Records relating to user names, passwords, screen shots, e-mails, or other information that appears to have been obtained from computers operated or controlled by Joe Kernell, Butch Kirven, or members of the Greenville County Council;
- c. Records relating to "Remote Spy," remotespionage.com, or spy software;
- d. Correspondence in any form pertaining to the unauthorized access to a computer;
- e. Records evidencing ownership or control of any computer or other data storage media seized pursuant to this warrant;
- f. Records relating to or embodying passwords, password files, test keys, encryption codes, or other information necessary to access computer equipment, storage devices, or data seized pursuant to this warrant

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as hard disks, thumb drives, or other media that can store data); any handmade form (such as writing, drawing, painting); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies).